REMARKS

Claims 1-38 are present in this application including independent claims 1, 23, 24 and 29. Claims 2 and 4 have been canceled and the features recited therein have been incorporated into amended claims 1 and 23. Claim 25 has been canceled and the features recited therein have been incorporated into amended claim 24. Thus, the claims recite that the plurality of nodes include a verifying node coupled to a new entity for verifying the identification of the new entity into the hybrid authentication system and that the verifying node signs a certificate related to the new entity. No new matter has been added, and no new issues are presented that require further search and/or consideration.

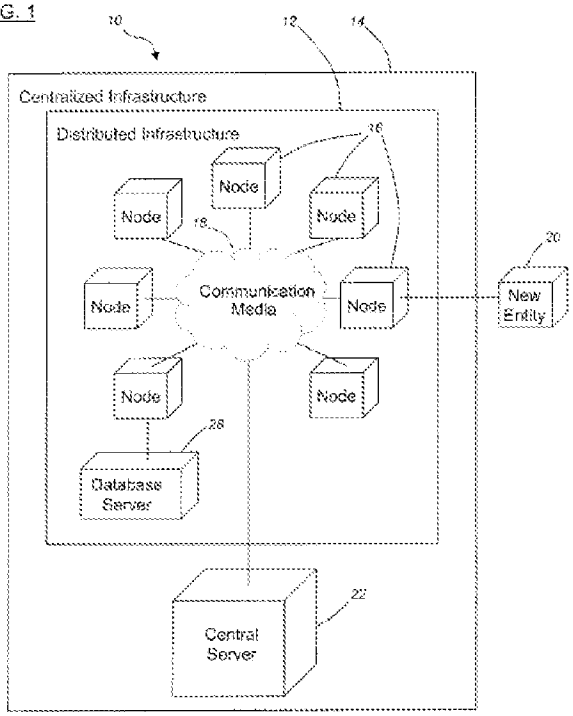
The Examiner has repeated his rejection of the claims as was previously set forth in the office action of November 5, 2007.

The applicant's invention can be at its simplest described as a hybrid authentication system for securing communication comprising a distributed authentication infrastructure with a series of interconnected nodes, which nodes are provided for performing a series of functions, including the authentication of other nodes. The system also includes a centralized authentication system infrastructure which is later integrated into the distributed authentication infrastructure after establishment of the distributed authentication infrastructure. The centralized authentication infrastructure includes a central server coupled to the nodes for verifying the identification of the nodes and/or granting permission to those nodes. As a result of the centralized infrastructure, the nodes can receive support from the central server in enrollment, authentication, permission, etc. tasks. An important feature of the applicant's system is for example in connection with enrolling a new entity into the system and therefore whether the new

entity can have access to data transferred or stored in the system. This is accomplished by requiring the new entity to present a certificate of one or more predetermined credentials to one or more nodes. (*see* paragraph 0056 and Fig. 6).

The applicant's invention can be appreciated from the following (Fig. 1 of the application).

FIG. 1



The Examiner has rejected claims 1-3, 7, 11, 13-14, 18, 22-24, 29-34 and 36 under 35 U.S.C. 102(e) as anticipated by Leoutsarakos (U.S. 2004/0039905) (hereinafter Leo). Applicant respectfully requests reconsideration of this rejection.

It is the Examiner's position with respect to independent claim 1 that "Leo discloses a distributed authentication infrastructure including a plurality of nodes in communication with each other, each of said plurality of nodes having an identification

and intended to perform a series of functions, one of said series of functions for verifying said identification of said plurality of nodes." The Examiner relies on figures 1 and 7.

It is submitted that Leo does not teach the invention of any of the independent claims as now amended and in particular as to the feature of requiring a new entity to present a certificate of one or more predetermined credentials to the nodes and whereby the node(s) can determine whether the new entity is privileged for enrolment. This feature is not present in Leo and therefore Leo can not anticipate the instant invention.

The rejection of claim 1 should therefore be withdrawn.

Claims 23, 24 and 29 are independent claims and have similar limitations as those of claim 1. The rejection of these claims under 35 U.S.C. 102(e) as anticipated by Leo should also be withdrawn. Dependent claims 3, 7, 11, 13-14, 18, 22, 30-34 and 36 have similar limitations as those of claim 1 and therefore their rejection under 35 U.S.C. 102(e) is similarly improper and should be withdrawn.

The Examiner has rejected claims 8 and 38 as unpatentable under 35 U.S.C. 103(a) over Leo in view of Dinker. Applicant respectfully requests reconsideration of this rejection.

The Examiner admits that Leo "does not disclose wherein said distributed authentication infrastructure requires a quorum of said plurality of nodes for enrolling a new entity into the hybrid authentication system" and relies on Dinker as disclosing "the quorum of said nodes for enrolling a new entity," concluding that "it would have been obvious to one of ordinary skill in the art to apply the quorum method of Dinker into the

system of Leo to enhance security because the pre-selected nodes have to vote and agree with each other in order for the new entity (to) get enrolled into the system."

As set forth above, Leo does not teach all of the required limitations of the independent claims and specifically claim 1; claims 8 and 9 are dependent claims directed to very specific features alleged to be found in Dinker. However, Dinker does not teach or suggest the required limitations of claim 1. Therefore the combination of Leo and Dinker fails to render the applicants' invention as set forth in dependent claims 8 and 38 obvious. It should be noted that Dinker is directed to an entirely different system and as described operates so that in cluster 100 (group of nodes) which is configured to interact with one or more external clients (110 Fig 1A and 140 Fig. 1B) coupled to the cluster 100 via network 130 and during the interaction of the cluster 100 with clients, the clients may send the cluster requests for access to services provided by and/or data stored in the cluster, or request write access to update data already stored in the cluster or to create new data within the cluster. Each node includes a consensus module and a serviceability module. In response to receiving a request to perform a serviceability update, a consensus module will send a vote to each other consensus module and depending on whether a quorum is indicated by the votes received from the consensus modules in the other nodes the serviceability module will perform the serviceability update. The skilled in the art would not consider making the modification to Leo as suggested by the Examiner because of the differences in subject matter and if he did, he would still, because of the differences in Leo from the claimed invention, not achieve the applicant's invention as claimed.

The Examiner has rejected claim 12 (35 U.S.C. 103(a)) over Leo in view of Prabandham. Applicant respectfully requests reconsideration of this rejection.

It is noted that claim 12 is a dependent claim drawn to a preferred feature. The Examiner has conceded that "Leo does not disclose in details wherein said control server is coupled to a new entity and is utilized for verifying the identification of the new entity and enrolling said new entity into the hybrid authentication system, said central server producing a log for recording a plurality of failed authentication and a plurality of failed enrolments by said plurality of nodes" and relies on Prabandham to cure the omission. As Prabandham does not teach the elements of claim 1, it can not cure the deficiencies of Leo and therefore the rejection of claim 12 should be withdrawn.

Claims 4-6, 15-17, 19-21, 25-28, 35 and 37 have been rejected under 35 U.S.C. 103(a) over Leo in view Benatar. Applicant respectfully requests reconsideration of this rejection. Again these claims are all dependent claims.

The Examiner has rejected claims 9-10 under 35 U.S.C. 103(a) as being unpatentable over Leo in view of Dinker and further in view of Benatar. Applicant respectfully requests reconsideration of this rejection. In connection with the rejection of the dependent claims 9 and 10, the Examiner admits that Leo does not explicitly disclose wherein each node of said quorum utilizes a partial key for partially signing a certificate related to said new entity so as to provide said new entity with a full signature" and relies on Benatar and Dinker to cure this omission. As noted above, Leo fails to disclose all the limitations of the independent claim 1 and as neither Benatar nor Dinker cures these

deficiencies, this ground of rejection should be withdrawn. Again it is pointed out that it is the applicant's position that Benatar fails to teach what the Examiner relied on it to teach, i.e., "each node of said quorum utilizes a partial key for partially signing a certificate related to said new entity so as to provide said new entity with a full signature." The paragraphs cited by the Examiner in Benatar (0008, 0011 and 0037) are related to signing a certificate and no reference was made to each node of said quorum utilizing a partial key for partially signing a certificate to provide a full signature. (page 6 of amendment filed 2/5/2008).

Claim 10 depends on claim 9.

The Examiner should withdraw this ground of rejection.

In response to the Examiner's position (page 4 of the office action) that "one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references," what the applicant is attempting to show is that Leo, the primary reference, does not teach nor suggest all of the limitations of the independent claims, in particular claim 1, and that these limitations are not taught, suggested nor supplied by the secondary references, the latter being cited in connection with preferred features set forth in dependent claims. So that the combination of references would not render applicant's claims obvious.

In view of the above, withdrawal of the rejection of the claims and an indication of allowable subject matter are respectfully requested.

SUMMARY

It is submitted that the application is in condition for allowance and notification thereof is respectfully requested. Should any issue remain to be resolved, Applicant requests that the Examiner telephone the undersigned attorney of record.

Respectfully Submitted,
Attorney for Applicant

Dated: July 2, 2008

/evelyn m. sommer/

Evelyn M. Sommer
Registration No. 19,603
Joshua S. Broitman
Registration No. 38,006
OSTRAGER CHONG FLAHERTY AND BROITMAN, PC
570 Lexington Avenue, 17th Floor
New York, NY 10022-6894
Phone: (212) 681-0600
Customer Number: 64722